

# Proposal to Reduce Identity Theft with Personal Identification Numbers

By Mark Peters

August 8, 2003 (Last revised November 21, 2003)

Latest Version: <http://www.thepeters.org/IdTheftPrevention.htm>

PDF Version: <http://www.thepeters.org/IdTheftPrevention.pdf>

## Abstract

This paper proposes a simple solution for stopping identity theft by allowing consumers to request and provide a per-credit-application personal identification number (PIN) every time they authorize credit to be extended in their name. Creditors who did not provide the assigned per-application PIN at the time credit was extended will be barred from reporting any credit events on the consumer's credit report. This should greatly minimize damage done when a Social Security number (SSN) is compromised and misused, because the credit report will remain untarnished and legitimate credit applications will continue to be permitted.

## The Problem

The main problem is that creditors extend credit with only a cursory validation that the person requesting credit is truly who he or she purports to be. As a result, identity thieves who provide the wrong name, incorrect addresses, other incorrect background information are often still successful in impersonating the identity theft victim. Furthermore, savvy identity thieves can obtain and provide correct information so that a creditor cannot distinguish and identity thief from the real person.

The Federal Trade Commission reports that there were 162,000 actual identity theft cases reported to them in 2002, and this is thought by many market research firms to be a fraction of the actual number of cases. Testimony for HR 4311 indicates that there were over 500,000 actual cases per year in 1999 and that each case cost the consumer an average of \$17,000 to resolve. That's \$8.5 Billion dollars per year that innocent individuals end up spending to begin to straighten up their lives, and untold billions in financial losses borne by the creditors.

SSNs were not originally intended to be used for the breadth or purposes seen today. SSNs are used for medical insurance, blood donations, driver's license applications, loan and credit applications, a variety of required college entrance forms, tax filings, and numerous other uses.

The SSN is treated by creditors as some secret that, once provided, grants the identity thief access to the remaining viable credit of the victim. However, there are hundreds of people who have seen the SSN of an individual during his or her lifetime. Additionally, there are people who have access to systems which will look up someone's SSN in government and in credit departments of private corporations. Given all of this, it is clear that *an SSN can hardly be considered a secret for the purposes of applicant authentication*

Also contributing to the problem is the credit bureaus' stance that they are merely "reporters of information". Credit bureaus compound the problem because they do not authenticate debtors and will gladly report false information about a debtor as long as a creditor provides them with this information. The only way that the known identity theft problem can be fixed is for the credit bureaus to step up and participate in the solution to report only authenticated credit events.

## **A Simple Solution**

I propose that consumers should be allowed to request a secret personal identification number (a master PIN). When that consumer applies for credit, he or she uses the master PIN to call or web-browse to an automated system to get a per-application PIN for a particular credit application. The creditor may only use the per-application PIN for the purpose of requesting a credit report and later reporting credit events directly related to the subject credit application. Subsequent credit applications would require a new per-application PIN. The only time the consumer uses the per-application PIN is during the initial credit application. The creditor retains the per-application PIN if it wishes to later report credit events for this credit account.

It is even possible to come up with a system with more sophisticated protection years down the road. For example, the consumer could be given the option to restrict the use of the per-application PIN. For example, the consumer might specify that the per-application PIN is to be used for a general credit card, store credit card, car loan, or mortgage as well as provide the maximum credit limit or loan amount. The consumer may also specify an expiration date by which time the credit report must be requested for said purpose. Additionally, the consumer might provide a creditor identification number assigned by the central authority to keep the per-application PIN from being used by an unauthorized creditor, as well as permit correlation between events reported by various credit bureaus.

The master PIN & per-application PIN scheme is not new. It is currently being used by companies for employment verification when applying for mortgages, etc. I am not aware if any of this proposal might be covered by patents.

## **Implementation**

The solution may be simple, but the challenge is going to be motivating the right parties.

## The Players

- **Consumers** are the ones getting shafted. They are clearly fed up with the broken system which provides a fertile breeding ground for identity theft. Those who want more protection can opt-in to this scheme. Those who don't will opt-out by default.
- **Credit Bureaus** currently collaborate to centralize the consumer "solicitation opt-out requests". In the U.S., there are three main credit bureaus. This scheme would be centralized in the same manner as it would be too burdensome for consumers to manage multiple master PINs. These bureaus have a duty to ensure that the information they manage and sell is correct. They also have an obligation to limit access to appropriate entities. These bureaus want to minimize operating expenses, so motivation will likely take the form of FTC or legislative mandates or by consumers paying for this service. One de-motivator for bureaus to implement this proposal is that they make money by selling credit reports and credit change notification services to consumers who fear identity theft and this proposal might decrease the need for those services. The credit bureaus help perpetuate this fear with advertising for their identity theft protection services.
- **Creditors** use credit reports to determine whether or not to grant credit. They wield the power of ruining a consumer's credit report, even in cases where the consumer did not authorize the credit. Creditors will be motivated by losing the right to post credit reports if the consumer's credit record required per-application PINs at the time the credit application was filed.

## Logistics

To apply this technique to identity theft prevention, every time new credit is being established where a consumer requires a per-application PIN, the applicant must request and provide an appropriate per-application PIN. To request a per-application PIN, the applicant calls the central authority and provides the master PIN. The applicant provides the per-application PIN in the credit application. The creditor provides the per-application PIN to its credit bureau when requesting the credit record and when reporting credit events. The credit bureau verifies each per-application PIN with the central authority.

To request the master PIN, the applicant could follow a process similar to the permanent solicitation opt-out process used today. For example, the applicant could call the central authority run jointly by the credit bureaus and provides detailed identifying information. The central authority mails a numbered, but otherwise blank form with no identifying information to the applicant. The applicant again provides identifying information on the form as well as the first two digits of the master PIN. A response is mailed to the applicant with the the remaining digits in the master PIN. One week later, a letter is mailed to the recent addresses on file indicating that the process is complete (but not providing any sensitive information). There are a number of variations to this process which would minimize risk. For example, the central authority could establish kiosks in metropolitan areas which require a photograph or thumbprint to secure the request. The master PIN could be issued immediately in these cases to prevent interception during mailing. Additionally, there could be a delay in activating the master PIN until adequate time has elapsed for someone to repudiate the issuance of the master PIN once the confirmation letter is received.

## Proposal to Reduce Identity Theft with Personal Identification Numbers

If the master PIN is reported lost or compromised by someone who can withstand an identification challenge, the credit record is frozen for new credit and the master PIN assignment process is repeated, preferably in a manner dictated by the consumer during the original request. Options include:

- Participation of notary public with the form mailed to the central authority.
- Calling into the central authority and providing additional authentication factors, such as:
  - Providing recent mortgage and loan payments
  - Originating the call from a known home or work number (using caller ID)
  - Providing other secret pre-arranged information

In addition, all recent creditors are notified of the potential breach.

Laws should be enacted imposing liability for creditors who fail to obtain a required per-application PIN when issuing a new credit line and for threatening a negative credit report when a per-application PIN was required but not provided. One form of liability is to disallow any claims against debtors by creditors if a PIN was not obtained for credit lines or loans where a credit check was performed. Furthermore, fines in this situation could be used for restitution of time and other expenses incurred by identity theft victims.

### **Funding**

Since the current process is clearly broken, I believe that the operation of this scheme should be funded by the bureaus through existing fees charged to creditors when requesting credit.

However, an alternative to this could be accomplished via user fees. These fees should be capped by law. A consumer might pay \$10 or \$20 for 10 years of master PIN service. Resetting of a lost or compromised master PIN could carry a fee. The central authority would be responsible for mailing renewal notices in a timely manner to known recent addresses to prevent lapse of this protection.

### **The Bottom Line**

Until some more comprehensive technological solution is in place, this simple solution should vastly improve the pitiful lack of protection for hundreds of millions of Americans who are at risk for identity theft. It may even cut down on title theft when fraudulent identity is used to obtain a mortgage.

---

## **SCENARIOS**

### **Scenario: Typical Credit Application with Per-Application PIN**

Joe is shopping for furniture. The store is currently offering a 6 month interest-free loan if the goods are charged to the store credit card. Joe doesn't have a store credit card, so he fills out the credit application. He notices that there is a place for a per-application PIN, so he calls the central authority, enters his identifier and master PIN as well as the store's creditor identifier. The system issues a per-application PIN and Joe writes it into his application. The store runs the credit report, providing the per-application PIN. The credit bureau verifies the per-application PIN with the central authority. As credit events occur, such as the initial credit line being extended and monthly billing, the creditor reports the events with the per-application PIN, and the bureau verifies these with stored records or with the central authority. Once the account is reported as closed, the per-application PIN is no longer valid and no further credit events may be reported.

When the central authority receives reports regarding the same per-application PIN from multiple bureaus, it must verify that the creditor and account identification matches. The first bureau to report with the per-application PIN is considered correct and the subsequent ones are rejected if the creditor identification does not match previous reports of record for that per-application PIN.

### **Scenario: Authenticated Credit Application Has Delinquent Payments**

Continuing the previous scenario, if Joe is delinquent in payment, the creditor reports the delinquency while providing the per-application PIN.

### **Scenario: Identity Theft Thwarted**

Fred impersonates Joe and tries to open a credit card account in Joe's name. The creditor runs a credit report without the per-application PIN and the credit report indicates that a per-application PIN is required. If the creditor chooses to grant credit anyway, then when it reports credit events without the per-application PIN, the credit events are denied by the credit bureau. Joe's credit does not show this negative credit event. Thus, Joe's credit is untarnished.

### **Scenario: Repudiation of Derogatory Reported Credit Event**

In the case that the credit bureau failed to respect the per-application PIN requirement, Joe could repudiate the reported derogatory credit events by either contacting each bureau in writing or by contacting the central authority with the repudiated event information.

If Joe reported an event for which a per-application PIN was in fact used, then Joe would pay an administrative fee to the central authority for his error.

If the bureau failed to respect the per-application PIN requirement in effect at the time the credit was extended, then it would pay an administrative fee to the central authority for its error, which the bureau might recover from the creditor. Furthermore, Joe would be entitled to recover damages for any losses incurred from the bureau and creditor.

### **Scenario: Transfer of Account to Another Creditor**

Consumer accounts are frequently sold to other financial institutions. The old creditor would to submit a "transfer account request" to the central authority with the per-application PIN and identify the new creditor.

### **Scenario: Creditor Changes Account Number**

Account numbers change for a variety of reasons, including financial institution mergers and account numbering expansions. Since the central authority would normally prohibit the per-application PIN from being used for an account number which differs from the originally reported one, the creditor would need to submit an "account number change request" with the per-application PIN to register this change. There is room for abuse here, but abuses should become obvious during repudiation, particularly if there changes to the account other than the account number, such as addresses, principles, collateral, account type, etc.

### **Scenario: Address Change Protected by Master PIN**

One form of identity theft involves adding addresses to the credit report for new credit. This would be protected by per-application PINs for new credit. Another form of identity theft called "account hijacking" involves changing an existing account to a new address to hide fraudulent activity. Sometimes new accounts are created after an existing account is hijacked. As this the implementations of this proposal mature, perhaps a "per-new-address PIN" or "per-move PIN" feature could be added to protect these situations.

#### **Scenario: Alternative "Lazy Reporting" to Central Authority**

The fundamental goal of this proposal is to minimize the effects of unauthorized abuse of a consumer's credit history. While the best approach is for each bureau to proactively report credit applications to the central authority, an alternate approach is for the bureaus not to report credit applications and events to the central authority, but to immediately remove derogatory credit events which do not have required per-application PINs upon repudiation by the debtor. Note that events prior to the per-application PIN being set up on a particular debtor's credit report would remain on the credit report and would not be permitted to be repudiated via this mechanism.

---

### **Considerations regarding consumer-specified per-application PIN restrictions**

It may not be wise to allow restrictions on the credit limit amount for long term credit card

relationships. It would be nice to have this to prevent a credit card thief from bumping up the credit card limit. But it would likely cause problems in many cases where automatic increases are in play. It would also complicate whether the credit card issuer is allowed to post derogatory events if the issuer failed to get a per-application PIN to increase the credit line.

### **Further Items needing consideration...**

The "bad check scenario" needs to be further considered. This is the case where a credit check was not run by bank ahead of time. Checking accounts apparently do not require a credit check, so banks would be precluded from reporting in this scenario. Of course, if the account was created with identity theft or if an existing account was compromised by an impersonator, then precluding reporting would not be a bad thing. One might argue that a merchant filing charges (and winning the case) would be a sufficient reporting mechanism.

---

## **RISKS**

Every scheme has its risks, the devil is in the details, and security is not absolute. Almost any scheme is an improvement over the credit reporting status quo, but the success of this proposal will be based on balancing the security with impositions placed on consumers. Since this proposal would be adopted at the option of each consumer, these are the risks that each consumer must weigh when deciding to opt-in to per-application PINs.

Here are risks that the implementation needs to mitigate:

- **A Consumer's Master PIN is compromised**
  - **Master PIN is discovered by thief.** Individuals must memorize and protect their master PIN. There must be a way to freeze the report upon discovery of compromised master PIN.
  - **Master PIN is established by imposter.** The consumer would detect this by being denied credit for not providing a per-application PIN (when the consumer had never requested a master PIN). The consumer must be appropriately authenticated. The PIN application and assignment process must be sufficiently secure. There must be a way to freeze the report upon discovery of compromised master PIN.
  - **Master PIN is discovered via Attack.** The central authority must balance retries and availability. For example, three retries might cause a 4 hour delay before another 3 attempts are permitted. Then the window increases. A patient attacker could keep retrying until permanently locked out. A persistent attacker may eventually get lucky. An aggressive attacker could just keep trying random consumer identifiers and master PINs

until he gets lucky. Hopefully the caller ID trail would dissuade attackers of this nature.

- **Master PIN denial of service**

- **Master PIN is retried until blocked.** If an attacker exhausts the permitted retries of a particular consumer's master PIN, then when the consumer legitimately attempts to use the master PIN, the master PIN will be unusable and will have to be reset. This will cause the consumer to be inconvenienced and might cause an opportunity to be missed. Arguably, the consequences of having to reset the master PIN are more desirable than being a victim of a heinous case of identity theft. Customers should be contacted when their master PIN is revoked to minimize this risk.

- **Central Authority is compromised**

- **Central Authority is coaxed into giving out per-Application PINs.** If an attacker breaks into the system and bypasses use of the master PIN to grant single use PINs, then bogus credit events could be reported and legitimate repudiations would fail.
- **Fraudulent "past events" are inserted after the fact in the Central Authority's audit log.** Legitimate repudiations would fail because the bogus past events would appear to be legitimate. There are ways to mitigate this risk with secure auditing techniques.

## Useful Links

- [How Credit Reports Work](#)
- [Federal Trade Commission](#)
- [Testimony- House Ways and Means, SSN Subcommittee, July 10, 2003](#)
- [H.R. 4311—THE IDENTITY THEFT PREVENTION ACT OF 2000](#)
- [EPIC's report on cost of lack of privacy](#)
- [Privacy Rights organization](#)
- [Identity Theft Resource Center](#)
- [Identify Theft Prevention and Cure](#)
- [Crypto-Gram newsletter](#)